IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A seed generating circuit comprising:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data, wherein

the oscillating circuit has a first exclusive OR computing circuit, a first inverter circuit, a second exclusive OR computing circuit, and a second inverter circuit, coupled in series in this order,

data are given to one of input ends of the first exclusive OR computing circuit and to one of input ends of the second exclusive OR computing circuit, respectively, and

the oscillating circuit oscillates when the data inputted to the first and second exclusive OR computing circuits have a specific combination.

Claims 2-4 (Canceled).

Claim 5 (Original): The seed generating circuit according to claim 1, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated by the pseudo random number generating circuit.

Claim 6 (Original): The seed generating circuit according to claim 1, wherein appearance frequencies of "0" and "1" outputted from the smoothing circuit are more close to 1:1 than appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit.

Claim 7 (Original): The seed generating circuit according to claim 1, wherein the postprocessing circuit has an exclusive OR computing circuit which performs the computation.

Claim 8 (Original): The seed generating circuit according to claim 1, wherein the postprocessing circuit generates the one-bit seed based on a table which assigns either "0" and "1" corresponding to a combination of the plurality of bits.

Claim 9 (Currently Amended): A random number generating circuit comprising:

[[the]] a seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data, wherein

the oscillating circuit has a first exclusive OR computing circuit, a first inverter circuit, a second exclusive OR computing circuit, and a second inverter circuit, coupled in series in this order,

data are given to one of input ends of the first exclusive OR computing circuit and to one of input ends of the second exclusive OR computing circuit, respectively, and

the oscillating circuit oscillates when the data inputted to the first and second exclusive OR computing circuits have a specific combination.

Claim 10 (Original): The random number generating circuit according to claim 9, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated by the pseudo random number generating circuit.

Claim 11 (Original): The random number generating circuit according to claim 9, wherein the postprocessing circuit has an exclusive OR computing circuit which performs the computation.

Claim 12 (Original): The random number generating circuit according to claim 9, further comprising a uncertain logic circuit which gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.

Claim 13 (Currently Amended): A semiconductor integrated circuit comprising:

a random number generating circuit having:

[[the]] a seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data, wherein

the oscillating circuit has a first exclusive OR computing circuit, a first inverter circuit, a second exclusive OR computing circuit, and a second inverter circuit, coupled in series in this order,

data are given to one of input ends of the first exclusive OR computing circuit and to one of input ends of the second exclusive OR computing circuit, respectively, and

the oscillating circuit oscillates when the data inputted to the first and second exclusive OR computing circuits have a specific combination.

Claim 14 (Original): The semiconductor integrated circuit according to claim 13, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated by the pseudo random number generating circuit.

Claim 15 (Original): The semiconductor integrated circuit according to claim 13, further comprising a uncertain logic circuit which gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.

Claim 16 (Currently Amended): An IC card comprising:

a semiconductor integrated circuit including a random number generating circuit having:

[[the]] a seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data, wherein

the oscillating circuit has a first exclusive OR computing circuit, a first inverter circuit, a second exclusive OR computing circuit, and a second inverter circuit, coupled in series in this order,

data are given to one of input ends of the first exclusive OR computing circuit and to one of input ends of the second exclusive OR computing circuit, respectively, and

the oscillating circuit oscillates when the data inputted to the first and second exclusive OR computing circuits have a specific combination.

Claim 17 (Original): The IC card according to claim 16, further comprising a uncertain logic circuit which gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.

Claim 18 (Currently Amended): An information terminal equipment comprising:

~~the~~ a semiconductor integrated circuit including a random number generating circuit having:

[[the]] a seed generating circuit which generates a seed; and

a pseudo random number circuit which generates pseudo random, numbers based on the seed generated by the seed generating circuit,

the seed generating circuit having:

an oscillating circuit which oscillates continuously or intermittently, and which outputs a digital data sequence;

a smoothing circuit which outputs time series data by controlling appearance frequencies of "0" and "1" in the digital data sequence outputted from the oscillating circuit; and

a postprocessing circuit which generates one-bit seed by a computation using a plurality of bits included in the time series data, wherein

the oscillating circuit has a first exclusive OR computing circuit, a first inverter circuit, a second exclusive OR computing circuit, and a second inverter circuit, coupled in series in this order,

data are given to one of input ends of the first exclusive OR computing circuit and to one of input ends of the second exclusive OR computing circuit, respectively, and

the oscillating circuit oscillates when the data inputted to the first and second exclusive OR computing circuits have a specific combination.

Claim 19 (Original): The information terminal equipment according to claim 18, wherein the smoothing circuit includes:

a pseudo random number generating circuit which generates pseudo random numbers; and

a logical operation circuit which calculates an exclusive OR of the digital data sequence outputted from the oscillating circuit and the pseudo random numbers generated by the pseudo random number generating circuit.

Claim 20 (Original): The information terminal equipment according to claim 18, further comprising a uncertain logic circuit which gives a digital output which is not uniquely determined from a digital input value,

the pseudo random numbers are inputted into the uncertain logic circuit, and output from the uncertain logic circuit is outputted as a random number.